UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

ROBERT ANGULO, CHERIE KLEPEK DEANA SPAULDING, and SANDRA WEYERMAN, on behalf of themselves and all others similarly situated, Plaintiff, v. CENCORA, INC., and THE LASH GROUP, LLC Defendant.	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Robert Angulo, Cherie Klepek, Deana Spaulding, and Sandra Weyerman (together "Plaintiffs"), by and through their attorneys of record, upon personal knowledge as to their own acts and experiences, and upon information and belief as to all other matters, which Plaintiffs believe will be supplemented and supported after a reasonable opportunity for discovery, bring this class action complaint against defendants Cencora, Inc., ("Cencora") and the Lash Group, LLC ("Lash Group")(together "Defendants"), and allege as follows:

INTRODUCTION

1. Plaintiffs bring this class action on behalf of a Class, as defined below, against Defendants for their failure to properly secure and safeguard Plaintiffs' and Class Members' protected personal information stored within Defendants' information networks and servers, including, without limitation, "protected health information" ("PHI")[1] and "personally identifiable

[1] Protected Health Information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories, and data points applied to a set of demographic information for a particular patient. PHI is inclusive of and incorporates personally identifiable information.

information" ("PII"),[2] as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, PHI and PII are also referred to therein as "Private Information").

2. Cencora, based in Conshohocken, Pennsylvania, formerly known as AmerisourceBergen, is an American pharmaceutical company with over 46,000 employees worldwide.[3]

3. Lash Group, based in Conshohocken, Pennsylvania, provides consulting services and support for pharmaceutical, biotech and medical device companies as they evaluate and address reimbursement issues for their products.[4] Lash Group is owned by Cencora.[5]

4. In the course of providing their services, Defendants acquired and collected Plaintiffs' and Class Members' Private Information. Defendants knew at all times material that they were collecting, and responsible for the security of sensitive data, including Plaintiffs' and Class Members' highly confidential Private Information. This Private Information remains in the possession of Defendants, despite the fact that it was accessed by unauthorized third persons, is currently being maintained without appropriate and necessary safeguards, independent review, and oversight, and therefore remains vulnerable to additional hackers and theft.

5. Plaintiffs seek to hold Defendants responsible for the harms it caused and will continue to cause Plaintiffs and other similarly situated persons by virtue of a preventable

---

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[3] See https://www.cencora.com/newsroom/press-releases/amerisourcebergen-becomes-cencora (last visited July 3, 2024).

[4] See https://www.lashgroup.com/who-we-are (last visited July 3, 2024).

[5] See https://www.lashgroup.com/ (last visited July 3, 2024).

cyberattack on one of their vendor networks that occurred on February 21, 2024 (the "Data Breach").[6]

6. As a consequence, the Private Information that Defendants were entrusted with and responsible for, was accessed. This Private Information is significantly valuable to data thieves. Plaintiffs further seek to hold Defendants responsible for not ensuring that the Private Information was maintained in a manner consistent with industry standards.

7. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiffs' and Class Members' Private Information. The Data Breach occurred because Defendants maintained Class Members' Private Information in a reckless manner, and on their computer networks in a condition that was vulnerable to cyber-attack.

8. As a result of the Data Breach, the Private Information belonging to Plaintiffs and Class Members was lost. This PII included personal health information, such as names, date of birth, health diagnosis, and/or medications and prescriptions.[7]

9. Plaintiffs seek to hold Defendants responsible for not ensuring that Private Information, as defined by HIPAA Privacy Rule (45 CFR, Parts 160 and 164(A) and (E)), and respecting which Defendants was duty bound to protect pursuant to the HIPAA Security Rule (45 CFR, Parts 160 and 164(A) and (C)), was maintained in a manner consistent with industry standards, and other relevant standards.

10. HIPAA, in general, applies to healthcare providers and those health care providers that conduct certain health care transactions electronically, and HIPAA Business Associates, and sets standards for Defendants' maintenance of Plaintiffs' and Class Members' Private Information, including appropriate safeguards to be maintained by organizations such as Defendants' to protect

[6] See https://investor.amerisourcebergen.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=17314481 (last visited July 3, 2024).

[7] See https://www.lashgroup.com/notice (last visited July 3, 2024).

the privacy of patient health information, while setting limits and conditions on the uses and disclosures that may be made of such information without express customer/patient authorization.

11. Additionally, the so-called "HIPAA Security Rule" establishes national standards to protect individuals' electronic health information that is created, received, used, or maintained by a HIPAA Business Associate. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI. HIPAA provides the standard of procedure by which a medical provider must operate when collecting, storing, and maintaining the confidentiality of Private Information.

12. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants knowingly assumed legal and equitable duties to those individuals, including those arising from common law principles.

13. The risk of cyber-attack was well-known to Defendants and they were continuously on notice at all times material that their failure to take steps necessary to secure the Private Information from a risk of cyber-attack and unauthorized access left that information and property in a dangerous condition that was vulnerable to theft and misuse.

14. Although Defendants knew of the cyber-attack by no later than February 21, 2024, they failed to disclose the event, or otherwise provide their individual clients notice of the Data Breach.[8] Cencora did not update the public about the depth of the Data Breach until late May.

15. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations, as well as common law principles.

16. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable,

[8] *Supra*.

required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, upon information and belief, the Private Information of Plaintiffs and Class Members was compromised and damaged through access by and disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiffs and Class Members in the future – thus entitling them to damages. In addition, Plaintiffs and Class Members, who have a continuing interest in ensuring that their information is and remains safe, are entitled to injunctive and other equitable relief.

PARTIES

Plaintiff Robert Angulo

17. Plaintiff Robert Angulo is, and at all relevant times was, a resident of the state of Illinois, and a resident of Cook County.

18. Plaintiff Angulo provided substantial Personal Information, including, but not limited to, his name, address, date of birth, health diagnosis, and/or medications and prescriptions.

19. Plaintiff Angulo received a letter from Defendants, notifying him that his information had been accessed by third party actors.

20. According to this letter, Defendants learned that their data had been breached on February 21, 2024. On April 10, 2024, Defendants learned that Plaintiffs' information had been affected by this incident.

21. Plaintiff Angulo takes care in protecting his PII from disclosure. Faced with the risk of the unauthorized disclosure of her PII, he is now forced to monitor his accounts for signs of fraud and identity theft and devote valuable time and resources to same.

Plaintiff Cherie Klepek

22. Plaintiff Cherie Klepek is, and at all relevant times was, a resident of the state of Florida and a resident of Manatee County.

23. Plaintiff Klepek provided substantial Personal Information, including, but not limited to, her name, address, date of birth, health diagnosis, and/or medications and prescriptions.

24. Plaintiff Klepek received a letter from Defendants, notifying her that her information had been accessed by third party actors.

25. According to this letter, Defendants learned that their data had been breached on February 21, 2024. On April 10, 2024, Defendants learned that Plaintiffs' information had been affected by this incident.

26. Plaintiff Klepek takes care in protecting her PII from disclosure. Faced with the risk of the unauthorized disclosure of his PII, she is now forced to monitor her accounts for signs of fraud and identity theft and devote valuable time and resources to same.

Plaintiff Deana Spaulding

27. Plaintiff Deana Spaulding is, and at all relevant times was, a resident of the state of West Virginia and a resident of Mason County.

28. Plaintiff Spaulding provided substantial Personal Information, including, but not limited to, her name, address, date of birth, health diagnosis, and/or medications and prescriptions.

29. Plaintiff Spaulding received a letter from Defendants, notifying her that her information had been accessed by third party actors.

30. According to this letter, Defendants learned that their data had been breached on February 21, 2024. On April 10, 2024, Defendants learned that Plaintiffs' information had been affected by this incident.

31. Plaintiff Spaulding takes care in protecting her PII from disclosure. Faced with the risk of the unauthorized disclosure of his PII, she is now forced to monitor her accounts for signs of fraud and identity theft and devote valuable time and resources to same.

Plaintiff Sandra Weyerman

32. Plaintiff Sandra Weyerman is, and at all relevant times was, a resident of the state of Alabama and a resident of Randolph County.

33. Plaintiff Weyerman provided substantial Personal Information, including, but not limited to, her name, address, date of birth, health diagnosis, and/or medications and prescriptions.

34. Plaintiff Weyerman received a letter from Defendants, notifying her that her information had been accessed by third party actors.

35. According to this letter, Defendants learned that their data had been breached on February 21, 2024. On April 10, 2024, Defendants learned that Plaintiffs' information had been affected by this incident.

36. Plaintiff Weyerman takes care in protecting her PII from disclosure. Faced with the risk of the unauthorized disclosure of his PII, she is now forced to monitor her accounts for signs of fraud and identity theft and devote valuable time and resources to same.

Defendants Cencora and Lash Group

37. Cencora is a Delaware corporation with its headquarters located at 1 West First Avenue, Conshohocken, Pennsylvania 19428.

38. Cencora, formerly known as AmerisourceBergen, changed its name in 2023.[9]

39. Cencora's website claims that it is a "leading pharmaceutical solutions organization centered on improving the lives of people and animals everywhere."[10]

40. Lash Group is a division of Cencora, and is headquartered at 1 West First Avenue, Conshohocken, Pennsylvania 19428.

41. Lash Group provides consulting services and support for pharmaceutical, biotech and medical device companies as they evaluate and address reimbursement issues for their products.

42. Defendants collect and require their customers to provide PII in the course of providing their services.

43. By obtaining, collecting, using, and deriving benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties to those persons and knew, or should

[9] See https://www.businesswire.com/news/home/20230124005416/en/AmerisourceBergen-Announces-Intent-to-Change-Name-to-Cencora (last visited July 3, 2024).

[10] See https://www.cencora.com/who-we-are (last visited July 3, 2024).

have known, that they were responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure and/or criminal hacking activity.

JURISDICTION AND VENUE

44. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum value of $5,000,000.00, consists of putative class membership of greater than 100 members, and is a class action in which some of the members of the Class are citizens of states different than that of Defendant.

45. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant is authorized to conduct business within this District, is headquartered in this District, has intentionally availed itself of the laws in this District, and conducts substantial business, including acts underlying the allegations of this complaint, in this District.

FACTUAL BACKGROUND

Cencora and Lash Group's Business Involving the Collection and Maintenance of Private Background

46. Cencora provides pharmaceutical distribution services for doctor's offices, pharmacies, and animal healthcare.

47. Lash Group provides patient access services to pharmaceutical companies, including programs designed to ensure those patients are able to obtain pharmaceutical products.

48. As part of their distribution services, Defendants collected PII from their clients, including but not limited to their: personal health information, such as names, date of birth, health diagnosis, and/or medications and prescriptions.[11]

49. Defendants employ over 46,000 employees globally, services over ten million patients, and ships over 4 million products every day.[12]

[11] See https://www.lashgroup.com/notice (last visited July 3, 2024).

[12] See https://cencoraventures.cencora.com/about-cencora (last visited July 3, 2024).

50. Defendants require those persons and entities receiving their services – including their clients' patients – to provide their Private Information, which it is obligated to keep confidential and private.

51. Defendants acquired, collected, stored, and assured the security of, the Private Information of Plaintiffs and the Class.

52. Plaintiffs and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access. The information collected, acquired, and stored by Defendants included the Private Information of Plaintiffs and Class Members.

53. Plaintiffs and Class Members relied on the sophistication of Defendants to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members, who value the confidentiality of their Private Information and demand security to safeguard their Private Information, took reasonable steps to maintain the confidentiality of their Private Information.

54. At all times material, Defendants were under a duty to adopt and implement reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. To that end, Defendants were reposed with a legal duty created by HIPAA, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

55. By obtaining, collecting, using, and storing Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure. And given the highly sensitive nature of the Private Information they

possessed and the sensitivity of the medical and health services they provided, Defendants had a duty to safeguard, protect, and encrypt Plaintiffs' and Class Members' Private Information.

56. Defendants retain and store this Private Information and derive a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiffs' and Class Members' Private Information, Defendants would be unable to perform their services.

57. Defendants' failure to adequately safeguard the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

58. Defendants were not permitted to disclose Plaintiffs' and Class Members' Private Information for any reason that would apply in this situation.

59. Defendants were obliged by contract, industry standards, common law, and promises and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and protect it from unauthorized access and disclosure.

60. Plaintiffs and Class Members had a reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep the Private Information they provided confidential and secure from unauthorized access and disclosure.

61. Defendants' own Privacy Policy expressly comforts clients and their patients with the representation that "[w]e adopt appropriate security measures to protect the Personal Data we process, including sensitive Personal Data. We do not expect that our processing of sensitive Personal Data would impact your rights and interests adversely."[13]

[13] See https://www.cencora.com/global-privacy-statement (last visited July 3, 2024).

The Data Breach

62. On February 27, 2024, Cencora filed an 8-k disclosing that a cybersecurity incident had occurred, and that it had learned that unauthorized activity was detected on February 21, 2024.[14]

63. On May 20, 2024, Lash Group filed a notice of data breach with various state Attorney General offices after discovering that personal information provided to the company had been accessed by unauthorized users.

64. According to these notices, Defendants completed their investigation into the Data Breach by April 10, 2024.

65. Beginning in late May, Defendants began sending out data breach notice letters to individuals who were affected by the Data Breach.

66. As a result, Defendants knew that the data they had been protecting had been compromised, but failed to inform the public for several months. Even when Defendants had completed their investigation, it still took over a month for Defendants to notify affected individuals.

67. Defendants failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, consequently enabling and causing the exposure of Private Information of thousands of individuals.

68. Because of Defendants' negligence and misconduct in failing to keep the accessed information confidential, the unencrypted Private Information of Plaintiffs and Class Members have been expropriated by unauthorized individuals who can now exploit the PHI and PII of Plaintiffs and Class Members and use it as they please.

[14] See https://www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/1140859/000110465924028288/tm247267d1_8k.htm (last visited July 3, 2024).

69. Plaintiffs and Class Members now face a real, present and substantially increased risk of fraud and identity theft and have lost the benefit of the bargain they made with Defendants when receiving services.

70. As a consequence of Defendants' inadequate data security systems and protection, Plaintiffs and Class Members have been deprived of the benefit of their bargain which occurred when they agreed to receive services administered by Defendants. Plaintiffs and Class Members, reasonable consumers – understandably expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendants had not provided the necessary adequate data security in any event. Consequently, Plaintiffs and Class Members received services that were of a lesser value than what they had reasonably expected from and bargained for with Defendants.

Defendants' Business and Obligation to Preserve and Protect Confidentiality and Privacy

71. Defendants were entrusted with highly sensitive PII, including names, date of birth, health diagnosis, medication and prescription information, and other highly sensitive PII. Defendants retain and store this information and derive a substantial economic benefit from the Private Information that they collect.

72. Plaintiffs and Class Members are current or former clients of Defendants, or patients or employees of their clients, who obtained service(s) through Defendants.

73. Plaintiffs and Class Members provided their Private Information with the reasonable expectation and mutual understanding, either directly or as third party beneficiaries that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access, and Defendants expressly represented in their Privacy Policy that they would do so.[15]

[15] Supra; see also https://www.lashgroup.com/notice-of-privacy-practices (last visited on July 3, 2024).

74. Plaintiffs and Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members, who value the confidentiality of their Private Information and demand security to safeguard their Private Information, took reasonable steps to maintain the confidentiality of their PII.

75. Defendants derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. In addition, obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties, and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

76. At all times material, Defendants were under a duty to adopt and implement reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. And to that end, Defendants also had a legal duty created by contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure. Given the highly sensitive nature of the PII they possessed and the sensitivity of the services they provided, Defendants had a duty to safeguard, protect, and encrypt Plaintiffs' and Class Members' PII.

77. By obtaining, collecting, storing, and transmitting the Private Information of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

78. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendants to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

79. Defendants via their Privacy Policies expressly promised to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

80. Defendants' negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

81. Defendants were not permitted to disclose Plaintiffs' and Class Members' Private Information for any reason that would apply in this situation. The disclosure of Plaintiffs' and Class Members' Private Information via the Data Breach was not permitted per Defendants' own policies.

82. Defendants failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining of Plaintiffs and Class Members, consequently enabling and causing the exposure of Private Information in the Data Breach.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

83. The PII of consumers, such as Plaintiffs and Class Members, is valuable and has been commoditized in recent years.

84. Defendants were also aware of the significant repercussions that would result from their failure to do protect Private Information and knew, or should have known, the importance of safeguarding the Private Information entrusted to it and of the foreseeable consequences in the event of a breach of their data security. Nonetheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

85. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer both immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

86. As a direct and proximate result of Defendants' conduct, Plaintiffs and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must now be vigilant and continuously review their credit reports for suspected incidents of identity theft, educate themselves about security freezes, fraud alerts, and take steps to protect themselves against identity theft, which will extend indefinitely into the future.

87. Even absent any adverse use, consumers suffer injury from the simple fact that Private Information has been stolen. When such sensitive information is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the community.

88. Plaintiffs and the other Class Members also suffer ascertainable losses in the form of opportunity costs and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Purchasing credit monitoring and identity theft prevention;

C. Taking trips to banks and waiting in line to verify their identities in order to restore access to compromised accounts;

D. Placing freezes and alerts with credit reporting agencies;

E. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

F. Contacting their financial institutions and closing or modifying financial accounts;

G. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

H. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

I. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

89. Moreover, Plaintiffs and the other Class Members have an interest in ensuring that Defendants implement reasonable security measures and safeguards to maintain the integrity and confidentiality of the Private Information, including making sure that the storage of data or documents containing Private Information is not accessible by unauthorized persons, that access to such data is sufficiently protected, and that the Private Information remaining in the possession of Defendants is fully secure, remains secure, and is not subject to future theft.

90. As a further direct and proximate result of Defendants' actions and inactions, Plaintiffs and the other Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

91. As a direct and proximate result of Defendants' wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiffs' and other Class Members' Private Information, Plaintiffs and all Class Members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other personal accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed and exfiltrated in the Data Breach.

Defendants Were Well Aware of the Threat of Cyber Theft and Exfiltration in Healthcare Related Industries

92. As a condition of their relationships with their clients, customers, and Class Members, Defendants required that they entrust it with highly sensitive and confidential PII.

Defendants, in turn, collected that information and assured consumers that it was acting to protect that PII and to prevent its disclosure.

93. Defendants could have prevented the Data Breach by assuring that the Private Information at issue was properly secured.

94. Defendants' overt negligence in safeguarding Plaintiffs' and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as entities in the health, pharmaceutical and services industries, Defendants were on notice that such companies are targets for data breach hackers and cyber-thieves.

95. PII, including names and social security numbers are uniquely valuable to hackers. With these pieces of information, criminals can open new financial accounts in Class Member's names, take loans in their names, use their names to obtain medical services, obtain government benefits, file fraudulent tax returns in order to get refunds to which they are not even entitled, and numerous other assorted acts of thievery and fraud.

96. For this reason, hackers prey on companies that collect and maintain sensitive information, including medical institutions, insurers, and related entities. Companies like Defendants' have been aware of this, and the need to take adequate measures to secure their systems and information, for a number of years. In 2021 alone, approximately 330 breaches targeting healthcare providers occurred.[16] The steady growth of hacks of healthcare service providers is no surprise and can be tied to two significant factors, (1) the failure of healthcare services providers, like Defendants, to adequately protect patient data and (2) the substantial value of the sensitive PII entrusted to healthcare service providers.

[16] ITRC_2021_Data_Breach_Report.pdf (idtheftcenter.org) at 6. (last visited on July 3, 2024).

97. In the context of data breaches, healthcare is "by far the most affected industry sector."[17] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[18]

98. In 2021, 1,862 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, an increase of 68% over 2020 and a 23% increase over the previous all-time high.[19] These data breaches exposed the sensitive data of approximately 294 million people. *Id.*

99. Companies like Defendants are well aware of the risk that data breaches pose to consumers, especially because both the size of their customer base and the fact that the PII that they collect and maintain is profoundly valuable to hackers.

100. It can be inferred from the Data Breach that Defendants either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiffs' and Class Members' PII.

101. Upon information and belief, prior to the Data Breach, Defendants were aware of their security failures but failed to correct them or to disclose them to the public, including Plaintiffs and Class Members.

102. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendants knew or should have known that it did not make such actions and failed to implement adequate data security practices.

103. Because Defendants have failed to comply with industry standards, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is necessary to

---

[17] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed July 3, 2024).

[18] *Id.*

[19] See ITRC_2021_Data_Breach_Report.pdf (idtheftcenter.org) (last visited on July 3, 2024).

ensure Defendants' approach to information security is adequate and appropriate. Upon information and belief, Defendants still maintain the PII of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Representative Plaintiffs' and Class Members' PII remain at risk of subsequent data breaches.

104. In addition to their obligations under state and common laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the Private Information of Plaintiffs and Class Members.

105. Defendants owed a duty to Plaintiffs and Class Members to ensure that the Private Information they collected and were responsible for was adequately secured and protected.

106. Defendants owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII and financial information in their possession, including not sharing information with other entities who maintained sub-standard data security systems.

107. Defendants owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach that impacted the Private Information it collected and was responsible for in a timely manner.

108. Defendants owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

109. Defendants owed a duty to Plaintiffs and Class Members to disclose if their data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in their decision to entrust this Private Information to Defendants.

110. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

111. Defendants owed a duty to Plaintiffs and Class Members to mitigate the harm suffered by the Representative Plaintiffs and Class Members as a result of the Data Breach.

Defendants Violated FTC Guidelines Prohibiting Unfair or Deceptive Acts

112. The Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") prohibits businesses from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See e.g., FTC v. Wyndham Corp.*, 799 F.3d 236 (3d Cir. 2015).

113. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

114. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[21]

115. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

[20] See https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 3, 2024).

[21] See https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited July 3, 2024).

116. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

117. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

118. Defendants were at all times fully aware of their obligations to protect Plaintiffs' and Class Members' Private Information because of their business model of collecting Private Information and storing such information. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Conduct Fails to Adhere to Industry Standards, HIPAA and HITECH Standards, and Commensurate Duties it Owed to Plaintiffs and the Class

119. Defendants embraced a standard of care and commensurate duty defined by HIPAA, state law and common law to safeguard the PHI and PII of Plaintiffs and Class Members.

120. Moreover, Plaintiffs and Class Members surrendered their highly sensitive personal data under the condition and implied promise and assurance by Defendants that they would keep such Private Information confidential and secure. Accordingly, Defendants also had an implied duty to safeguard their data, independent of any statute.

121. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA.

These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

122. On information and belief, Defendants are considered a business associate pursuant to HIPAA.

123. Defendants are also regulated by the Health Information Technology Act ("HITECH"). See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

124. Because Defendants are covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

125. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

126. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

127. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

128. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

129. HIPAA's Security Rule requires Defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect Against reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by their workforce.

130. HIPAA also requires Defendants to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

131. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

132. Plaintiffs' and Class Members' Personal and Medical Information, including their PII and PHI, is "protected health information" as defined by 45 CFR § 160.103.

133. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

134. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

135. Plaintiffs' and Class Members' personal and medical information, including their PII and PHI, is "unsecured protected health information" as defined by 45 CFR § 164.402.

136. Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

137. Plaintiffs' and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

138. Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

139. Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

140. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

141. HIPAA requires covered entities and business associates to protect against reasonably anticipated threats to the security of sensitive patient health information.

142. Covered entities and business associates must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

143. This Data Breach constitutes an unauthorized access of PHI, which is not permitted under the HIPAA Privacy Rule.

144. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

145. The Data Breach could have been prevented if Defendants had implemented HIPAA mandated and industry standard policies and procedures for securely disposing of PHI

when it was no longer necessary and/or had honored their obligations to their patients with respect to adequately securing and maintaining the confidentiality of Private Information.

146. It can be inferred from the Data Breach that Defendants either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiffs' and Class Members' PII and PHI.

147. Upon information and belief, prior to the Data Breach, Defendants were aware of their security failures but failed to correct them or adequately and timely disclose them to the public, including Plaintiffs and Class Members.

148. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendants knew or should have known that they did not make such actions and failed to implement adequate data security practices.

149. Because Defendants failed to comply with industry standards, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is necessary to ensure Defendants' approach to information security is adequate and appropriate. Defendants still maintain the PII and PHI of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Plaintiffs' and Class Members' PII and PHI remains at risk of subsequent Data Breaches.

150. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the Private Information of Plaintiffs and Class Members.

151. Defendants owed a duty to Plaintiffs and Class Members to ensure that the Private Information they collected and were responsible for was adequately secured and protected.

152. Defendants owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in their possession, including not sharing information with other entities who maintained sub-standard data security systems.

153. Defendants owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach that impacted the Private Information they collected and were responsible for in a timely manner.

154. Defendants owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

155. Defendants owed a duty to Plaintiffs and Class Members to disclose if their data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in their decision to entrust this Private Information to Defendants.

156. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

157. Defendants owed a duty to Plaintiffs and Class Members to mitigate the harm suffered by the Representative Plaintiffs' and Class Members' as a result of the Data Breach.

158. Upon information and belief, Defendants' security failures include, but are not limited to:

e. Failing to maintain an adequate data security system and safeguards to prevent data loss;

f. Failing to mitigate the risks of a data breach and loss of data, including identifying internal and external risks of a security breach;

g. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants creates, receives, maintains, and transmits;

h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to

allow access only to those persons or software programs that have been granted access rights;

i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

j. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information;

k. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

l. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons; and

m. Retaining information past a recognized purpose and not deleting it.

Value of the Relevant Sensitive Information

159. The high value of PII to criminals is evidenced by the prices they garner on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[22] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[23] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[24]

160. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for

[22] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited July 3, 2024).

[23] *Id*.

[24] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited July 3, 2024).

COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

161. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

162. Identity thieves can use PII and financial information, such as that of Plaintiffs' and Class Members, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

163. The ramifications of Defendants' failure to keep secure Plaintiffs' and Class Members' PII are long lasting and severe. Once PII and financial information is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII of Plaintiffs and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

164. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

165. Data breaches are preventable.[26] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[27] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[28]

166. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[29]

Defendants' Delayed Response to the Breach

167. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of Plaintiffs and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII, especially their Social Security numbers, onto the Dark Web. Plaintiffs and Class Members

---

25 47 Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf (last visited July 3, 2024).

26 Lucy L. Thompson, Despite the Alarming Trends, Data Breaches Are Preventable, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

27 *Id*. at 17.

28 *Id*. at 28.

29 *Id.*

now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Medicare numbers, Social Security numbers, Dates of birth, and other critical PII.

168. Despite this understanding, Defendants did not timely inform affected individuals, including Plaintiffs and Class Members, about the Data Breach.

169. According to the letter that Plaintiffs received from Defendants, Defendants first learned of the Data Breach on February 21, 2024. Additionally, Defendants learned by April 10, 2024, that Plaintiffs were among the individuals affected by the Data Breach. Despite possessing this knowledge, Defendants failed to act on it by notifying Plaintiffs of the Data Breach until Defendants sent her a letter on May 21, 2024.

170. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.6% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[30]

171. According to the U.S. Bureau of Labor Statistics' 2022 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[31] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[32] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

---

30 U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, available at https://www.bls.gov/opub/reports/minimum-wage/2022/home.htm (last visited July 3, 2024); see also U.S. BUREAU OF LABOR STATISTICS, Employment And Average Hourly Earnings By Industry, available at https://www.bls.gov/news.release/empsit.t19.htm (last visited July 3, 2024) (finding that on average, private-sector workers make $1,166.20 per 40-hour work week).

31 See https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html?&qsearchterm=James%20Wallman (last visited July 3, 2024).

32 *Id.*

172. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

173. As a consequence of Defendants' inadequate data security systems and protection, Plaintiffs and Class Members have been deprived of the benefit of their bargain which occurred when they agreed to receive services administered by Defendants. Plaintiffs and Class Members, reasonable consumers – understandably expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendants had not provided the necessary adequate data security in any event. Consequently, Plaintiffs and Class Members received services that were of a lesser value than what they had reasonably expected from and bargained for with Defendants.

CLASS ALLEGATIONS

174. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert common law claims, as more fully alleged hereinafter, on behalf of the following Nationwide Class.

> **Nationwide Class**: All residents of the United States whose PII was accessed or otherwise compromised as a result of the Data Breach.

175. Alternatively, or in addition to the nationwide class, Plaintiffs seek to represent the following state classes.

> **Alabama Class**: All residents of the state of Alabama whose PII was accessed or otherwise compromised as a result of the Data Breach.
>
> **Florida Class:** All residents of the state of Florida whose PII was accessed or otherwise compromised as a result of the Data Breach.
>
> **Illinois Class**: All residents of the state of Illinois whose PII was accessed or otherwise compromised as a result of the Data Breach.
>
> **West Virginia Class**: All residents of the state of West Virginia whose PII was accessed or otherwise compromised as a result of the Data Breach.

Members of the Nationwide Class, the Alabama Class, the Florida Class, the Illinois Class and the

West Virginia Class are referred to herein collectively as "Class Members" or "Class."

176. Excluded from the Class are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

177. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

178. **Numerosity**: The exact number of members of the Class is unknown to Plaintiffs at this time but Defendants provide services to millions of consumers throughout the United States. Ultimately, members of the Class will be readily identified through Defendants' records.

179. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendants failed to adequately safeguard Plaintiffs' and the Class Members' Private Information;

b) Whether Defendants failed to protect Plaintiffs' and the Class Members' Private Information, as promised;

c) Whether Defendants' computer system systems and data security practices used to protect Plaintiffs' and the Class Members' Private Information violated federal, state, and local laws, or Defendants' duties;

d) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and the Class Members' Private Information properly and/or as promised;

e) Whether Defendants violated the consumer protection statutes, data breach notification statutes, state unfair practice statutes, HIPAA, state privacy statutes, and/or FTC law or regulations, imposing duties upon Defendants,

applicable to Plaintiffs and Class Members;

f) Whether Defendants failed to notify Plaintiffs and members of the Class about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

g) Whether Defendants acted negligently in failing to safeguard Plaintiffs' and the Class Members' Private Information;

h) Whether Defendants entered into contracts that included contract terms requiring Defendants to protect the confidentiality of Plaintiffs' Private Information and have reasonable security measures;

i) Whether Defendants' conduct described herein constitutes a breach of their contracts benefiting Plaintiffs and each of the Class Members;

j) Whether Defendants should retain the money paid by Plaintiffs and each of the Class Members to protect their Private Information;

k) Whether Plaintiffs and the Class Members are entitled to damages as a result of Defendants' wrongful conduct;

l) Whether Plaintiffs and the Class Members are entitled to restitution as a result of Defendants' wrongful conduct;

m) What equitable relief is appropriate to redress Defendants' wrongful conduct; and

n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Class Members.

180. **Typicality**: Plaintiffs' claims are typical of the claims of each of the Class Members. Plaintiffs and the Class Members sustained damages as a result of Defendants' uniform wrongful conduct during transactions with them.

181. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the Class, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Class, and there are no defenses

unique to Plaintiffs. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class.

182. **Separateness**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendants or would be dispositive of the interests of members of the proposed Class. Furthermore, the Private Information collected by Defendants still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the PII of Plaintiffs and Class Members.

183. **Class-wide Applicability**: This case is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Plaintiffs and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendants' practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiffs' challenge to those practices hinges on Defendants' conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiffs.

184. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendants' conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendants. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues

presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively the Alabama Class, and/or the Florida Class, and/or the Illinois Class and/or the West Virginia Class)

185. Plaintiffs, on behalf of themselves and the Class, re-allege and incorporate the above allegations by reference.

186. Plaintiffs and Class Members were required to submit PII to Defendants, in order to obtain services.

187. Defendants knew, or should have known, of the risks and responsibilities inherent in collecting and storing the PII of Plaintiffs and Class Members.

188. As described above, Defendants owed a duty of care to Plaintiffs and Class Members whose PII had been entrusted to Defendants.

189. Defendants breached their duty to Plaintiffs and Class Members by failing to secure the PII that Defendants collected from consumers from unauthorized disclosure to third parties.

190. Defendants acted with wanton disregard for the security of Plaintiffs' and Class Members' PII.

191. A "special relationship" exists between Defendants and the Plaintiffs and Class Members. Defendants entered into a "special relationship" with Plaintiffs and Class Members because it collected and/or stored the PII of Plaintiffs and the Class Members.

192. But for Defendants' wrongful and negligent breach of their duty owed to Plaintiffs and the Class Members, Plaintiffs and the Class Members would not have been injured.

193. The injury and harm suffered by Plaintiffs and Class Members were the reasonably foreseeable result of Defendants' breach of their duty. Defendants knew or should have known they were failing to meet their duty, and that Defendants' breach of such duties would cause

Plaintiffs and Class Members to experience the foreseeable harms associated with the unauthorized exposure of their PII.

194. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively the Alabama Class, and/or the Florida Class, and/or the Illinois Class and/or the West Virginia Class)

195. Plaintiffs, on behalf of themselves and the Class, re-allege and incorporate the above allegations by reference.

196. Pursuant to HIPAA (42 U.S.C. §1302d *et. seq.*), Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Personal Information.

197. Defendants breached their duties to Plaintiffs and Class Members under HIPAA (42 U.S.C. § 1302d *et. seq.*), by failing to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information, *i.e.*, by allowing Plaintiffs' Private Information to be taken without Plaintiffs' authorization by third parties.

198. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

199. But for Defendants' wrongful and negligent breach of their duty owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

200. The injury and harm suffered by Plaintiffs and Class Members were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duty, and that Defendants' breach of that duty would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the unauthorized access to their PII.

201. On information and belief, as a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively the Alabama Class, and/or the Florida Class, and/or the Illinois Class and/or the West Virginia Class)

202. Plaintiffs, on behalf of themselves and the Class, re-allege and incorporate the above allegations by reference.

203. Plaintiffs and Class Members entered into valid, binding, and enforceable express or implied contracts with entities affiliated with or serviced by Defendants, as alleged above.

204. The contracts respecting which Plaintiffs and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendants would act fairly and in good faith in carrying out their contractual obligations to take reasonable measures to protect Plaintiffs' PII from unauthorized disclosure and to comply with state laws and regulations.

205. A "special relationship" exists between Defendants and the Plaintiffs and Class Members. Defendants entered into a "special relationship" with Plaintiffs and Class Members who sought services from Defendants and, in doing so, entrusted Defendants, pursuant to their requirements and Privacy Notice, with their PII.

206. Despite this special relationship with Plaintiffs, Defendants did not act in good faith and with fair dealing to protect Plaintiffs' and Class Members' PII.

207. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Defendants.

208. Defendants' failure to act in good faith in complying with the contracts denied Plaintiffs and Class Members the full benefit of their bargain, and instead they received services that were less valuable than what they paid for and less valuable than their reasonable expectations.

209. Accordingly, on information and belief, Plaintiffs and Class Members have been injured as a result of Defendants' breach of the covenant of good faith and fair dealing respecting which they are express or implied beneficiaries, and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Breach of Duty
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively the Alabama Class, and/or the Florida Class, and/or the Illinois Class and/or the West Virginia Class)

210. Plaintiffs, on behalf of themselves and the Class, re-allege and incorporate the above allegations by reference.

211. Defendants accepted the special confidence placed in them by Plaintiffs and Class Members. There was an understanding between the parties that Defendants would act for the benefit of Plaintiffs and Class Members in preserving the confidentiality of their PII.

212. Defendants became the guardian of Plaintiffs' and Class Members' PII and accepted a fiduciary duty to act primarily for the benefit of their patients, including Plaintiffs and the Class Members, including safeguarding Plaintiffs' and the Class Members' PII.

213. Defendants breached their fiduciary duty to Plaintiffs and Class Members by (a) failing to protect the PII of Plaintiffs and the Class; (b) by failing to notify Plaintiffs and the Class Members of the unauthorized disclosure of the PII; and (c) by otherwise failing to safeguard Plaintiffs' and the Class Members' PII.

214. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiffs and/or Class Members have suffered and/or will suffer injury, including but not limited to: (a) the compromise of their PII; and (b) the diminished value of the services they received as a result of unauthorized exposing of Plaintiffs' and Class Members' PII.

215. On information and belief, as a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively the Alabama Class, and/or the Florida Class, and/or the Illinois Class and/or the West Virginia Class)

216. Plaintiffs, on behalf of themselves and the Class, re-allege and incorporate the above allegations by reference.

217. Defendants required Plaintiffs and the Class to provide and entrust their PII/PHI as a condition of obtaining medical care and medical devices from Defendants.

218. Plaintiffs and the Class paid money to Defendants in exchange for goods and services, as well as Defendants' promise or obligation to protect their protected health information and other PII from unauthorized disclosure.

219. Defendants promised and/or was bound by law to comply with HIPAA and HITECH standards and to make sure that Plaintiffs' and Class Members' protected health information and other PII would remain protected.

220. Through their course of conduct, Defendants, Plaintiffs, and Class Members entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII/PHI and financial information.

221. Defendants required Plaintiffs and Class Members to provide and entrust their PII/PHI, including for example, medical information, record or account numbers, names, dates of birth, and other information.

222. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII/PHI to Defendants, in exchange for, amongst other things, the protection of their PII/PHI. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

223. Plaintiffs and the Class Members would not have entrusted their PII/PHI to Defendants in the absence of Defendants' implied promise to adequately safeguard this confidential personal and medical information.

224. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

225. Defendants breached the implied contracts they made with Plaintiffs and the Class by making their PII/PHI accessible from the internet (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the PII/PHI was secure, failing to encrypt Plaintiffs and Class Members' sensitive PII/PHI, failing to safeguard and protect their medical, personal and financial information and by failing to provide timely and accurate notice to them that medical and personal information was compromised as a result of the data breach.

226. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to comply with their promise or obligation under the law to abide by HIPAA and HITECH.

227. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

228. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

229. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

230. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

231. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

232. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by their workforce violations in violation of 45 CFR 164.306(a)(94).

233. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

234. Defendants further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PII/PHI.

235. Defendants' failures to meet their promises and/or obligations constitute breaches of the implied contracts.

236. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) and/or actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) and/or the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

237. As a result of Defendants' breach of implied contract, Plaintiffs and the Class Members are entitled to and demand actual, consequential, and nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and the proposed Class, pray for relief and judgment against Defendants as follows:

A. certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure, appointing Plaintiffs as representative of the Class, and designating Plaintiffs' counsel as Class Counsel;

B. declaring that Defendants' conduct violates the laws referenced herein;

C. finding in favor of Plaintiffs and the Class on all counts asserted herein;

D. awarding Plaintiffs and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiffs and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiffs and the Class punitive damages;

G. awarding Plaintiffs and the Class civil penalties;

H. granting Plaintiffs and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendants from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiffs and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiffs and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: July 11, 2024

Respectfully submitted,

/s/ Andrew J. Heo
BARRACK, RODOS & BACINE
ANDREW J. HEO
JEFFREY W. GOLAN
Two Commerce Square
2001 Market Street, Suite 3300
Philadelphia, PA 19103
Telephone: (215) 963-0600
aheo@barrack.com
jgolan@barrack.com